KHIE
KENTUCKY HEALTH INFORMATION EXCHANGE

2013 Kentucky eHealth Summit

Karen Chrisman, JD, MA, CHP, CSCS
Governor's Office of Electronic Health Information

Kentucky
UNBRIDLED SPIRIT

KHIE
KENTUCKY HEALTH INFORMATION EXCHANGE

"This final omnibus rule marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."

HHS Office for Civil Rights Director, Leon Rodriguez

KHIE
KENTUCKY HEALTH INFORMATION EXCHANGE

45 CFR 160.130(3) Business Associate includes

(i) A Health Information Organization….

(ii) A person that offers a personal health record to one or more individuals….

(iii) A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the BA

45 CFR 160.308(b)

The Secretary may conduct a compliance review to determine whether a covered entity or business associate is complying with the applicable administrative simplification provisions in any other circumstance.

Civil Penalties

Up to $1.5 million fine	• Multiple violations due to willful neglect not corrected of an identical requirement or prohibition made during the same calendar year
$10,000 for each violation may not exceed $250,000	• Violation was due to willful neglect, corrected, violation of an identical requirement or prohibition during a calendar year

Civil Penalties

$1,000 for each violation may not exceed $100,000	• Violation was due to reasonable cause and not willful neglect of an identical requirement or prohibition during a calendar year
Up to $25,000 fine	• Single violation of a provision, or can be multiple violations with a penalty of $100 as long as each violation is for a different provision

Criminal Penalties

Up to $250,000 fine
up to 10 years
imprisonment

Wrongful disclosure of IIHI committed under false pretenses with intent to sell transfer or use for commercial advantage, personal gain, or malicious harm

Up to $100,000 fine
up to 5 years
imprisonment

Wrongful disclosure of individually identifiable health information committed under false pretenses

IIHI Individually Identifiable Health Information

Criminal Penalties

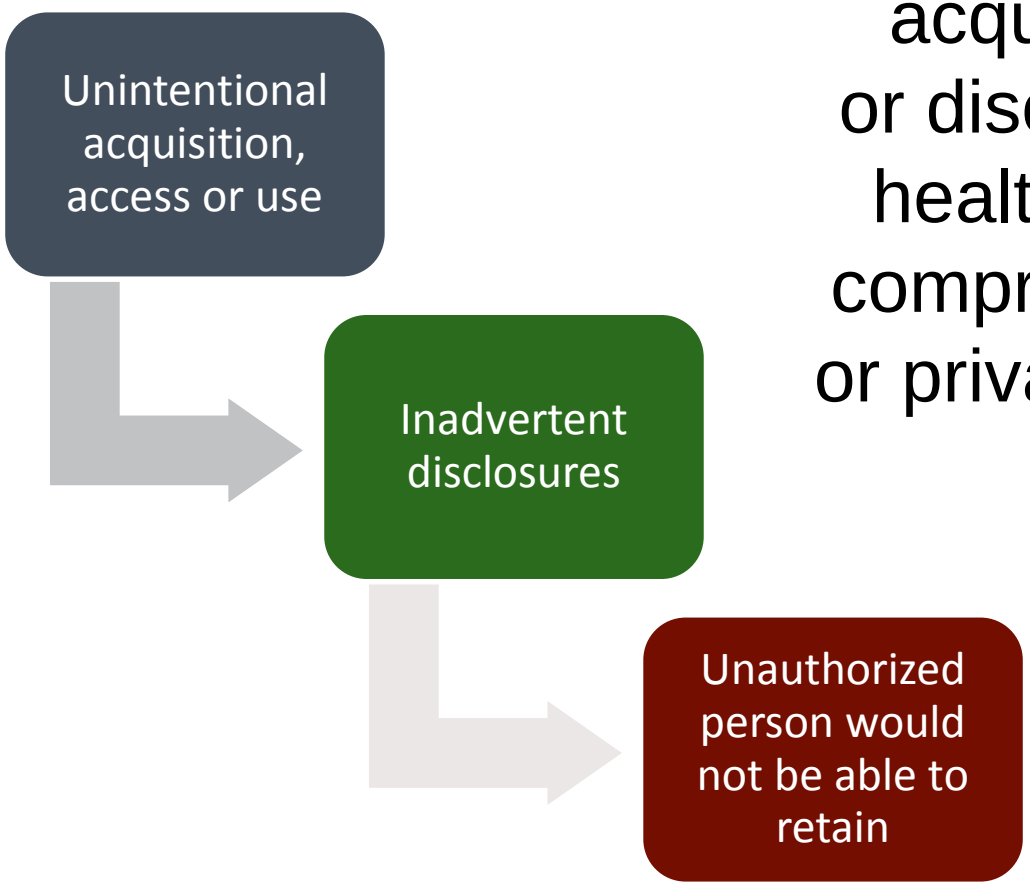
Up to $5O,000 fine

Up to 1 year imprisonment

Wrongful disclosure of individually identifiable health information

Breach by a Different Name

Three Exclusions



Breach means the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the protected health information.

Presumed to be a breach….

Unless the CE or BA demonstrates that there is a low probability the PHI is compromised based on a risk assessment of the following factors:

1. •The nature and extent of the PHI involved (identifiers and likelihood of re-identification)
2. • PHI actually acquired or viewed
3. • Extent the risk to PHI has been mitigated

<u>If PHI is encrypted there is no breach</u>

Burden of proving there is not a breach is on KHIE

Breach Criteria Met

Less than 500

- Notify HHS yearly, credit monitoring, notify patient

More than 500

- Notify HHS immediately, credit monitoring, notify patient
- Notify all local media outlets

$214.00 to $194.00 per record to remedy

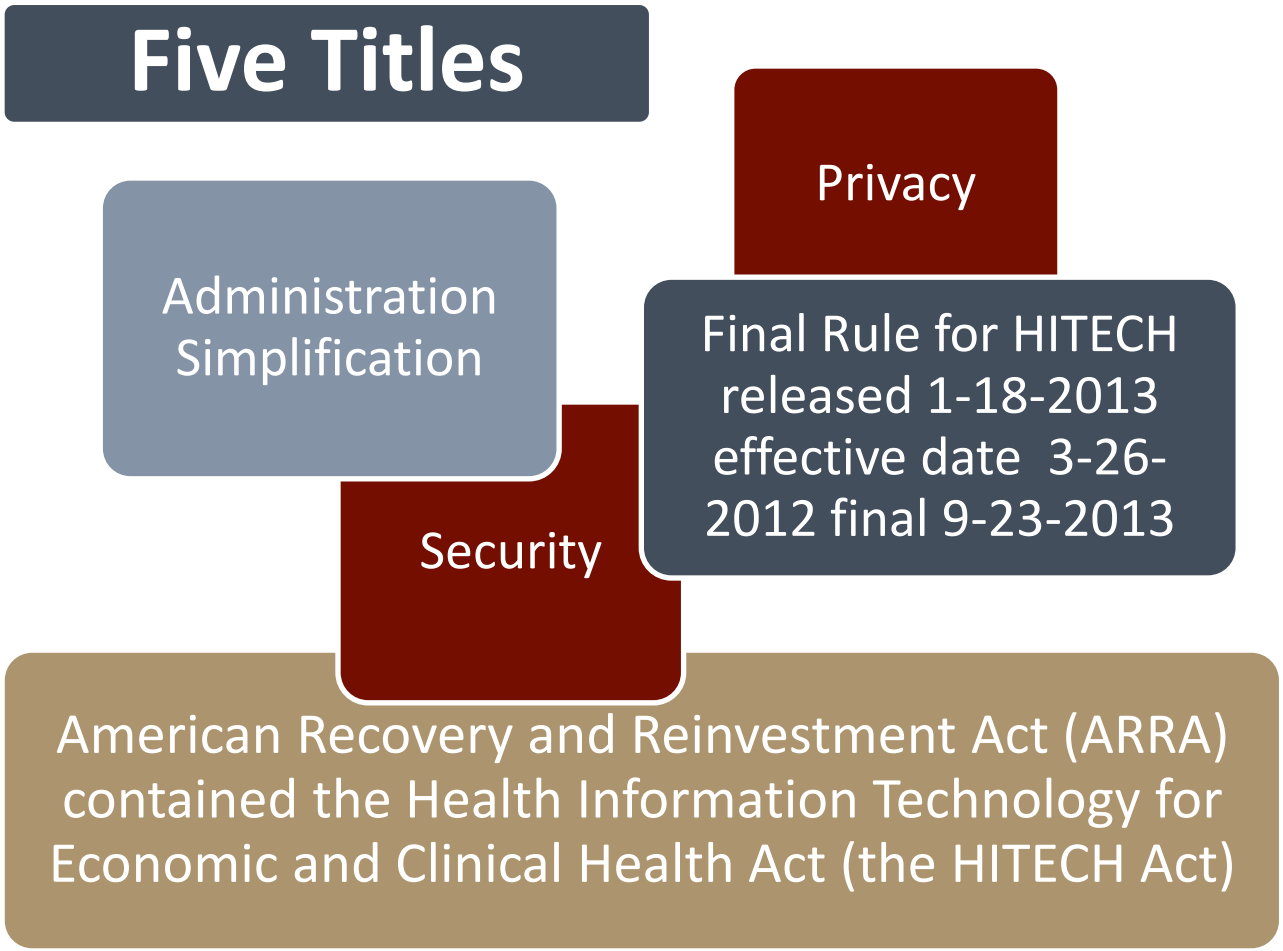
Data Breach Mop Up

Average cost per record of a data breach is $194.00 to $214.00 per record

Notification

Credit Monitoring

Health Insurance Portability and Accountability Act of 1996



Kentucky Data Breach 2010-2012

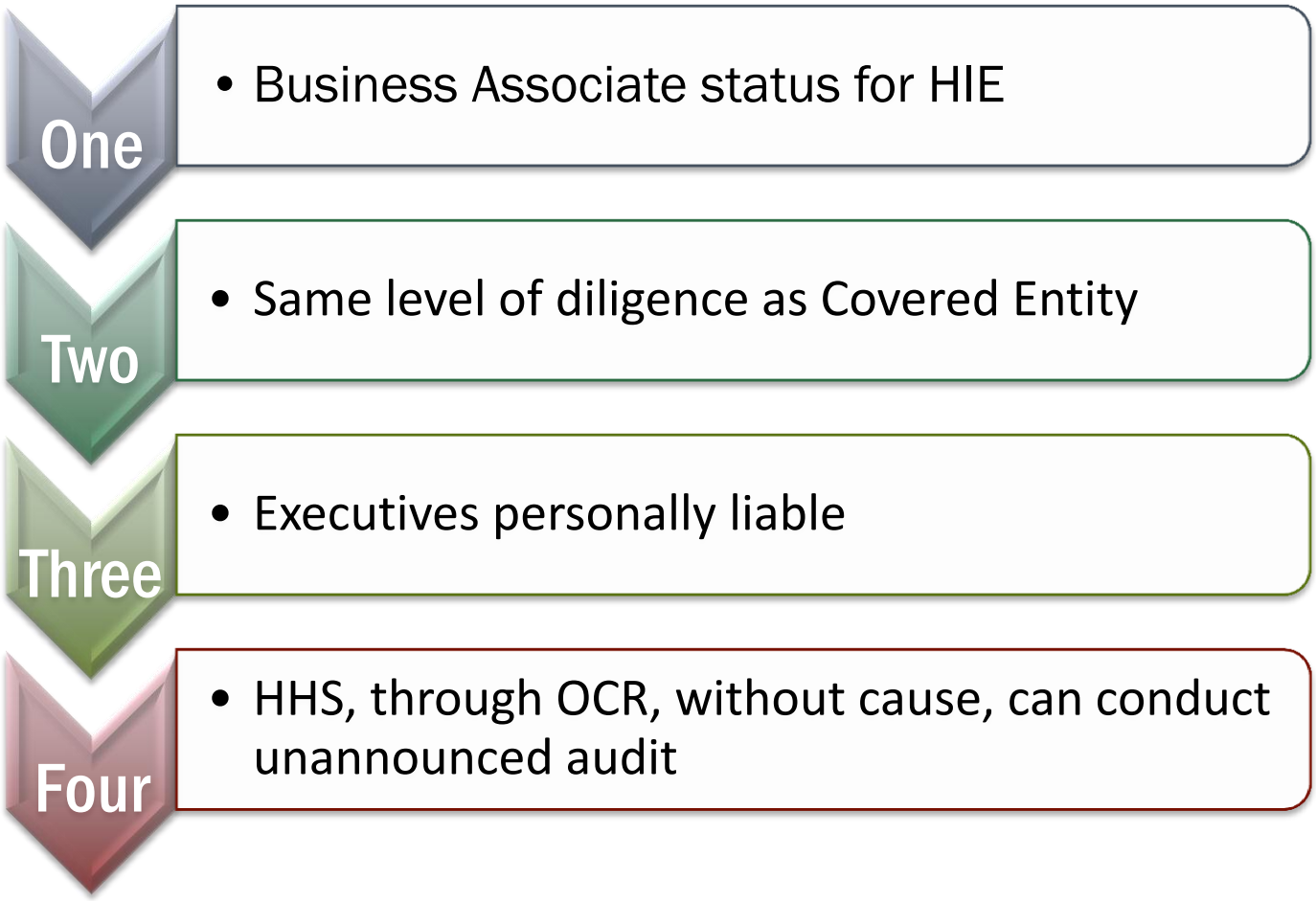
17 Kentucky incidents

Over 500 records required reporting to HHS

11 laptop or portable devices

78,844 patients affected

HITECH changed KHIE



Remained the same for KHIE

One

- KHIE can only use PHI for the purposes it was shared by the covered entity

Two

- KHIE must assume responsibility to safeguard PHI from misuse

Three

- KHIE must comply with covered entity's obligation to provide patient with access to their health information

Four

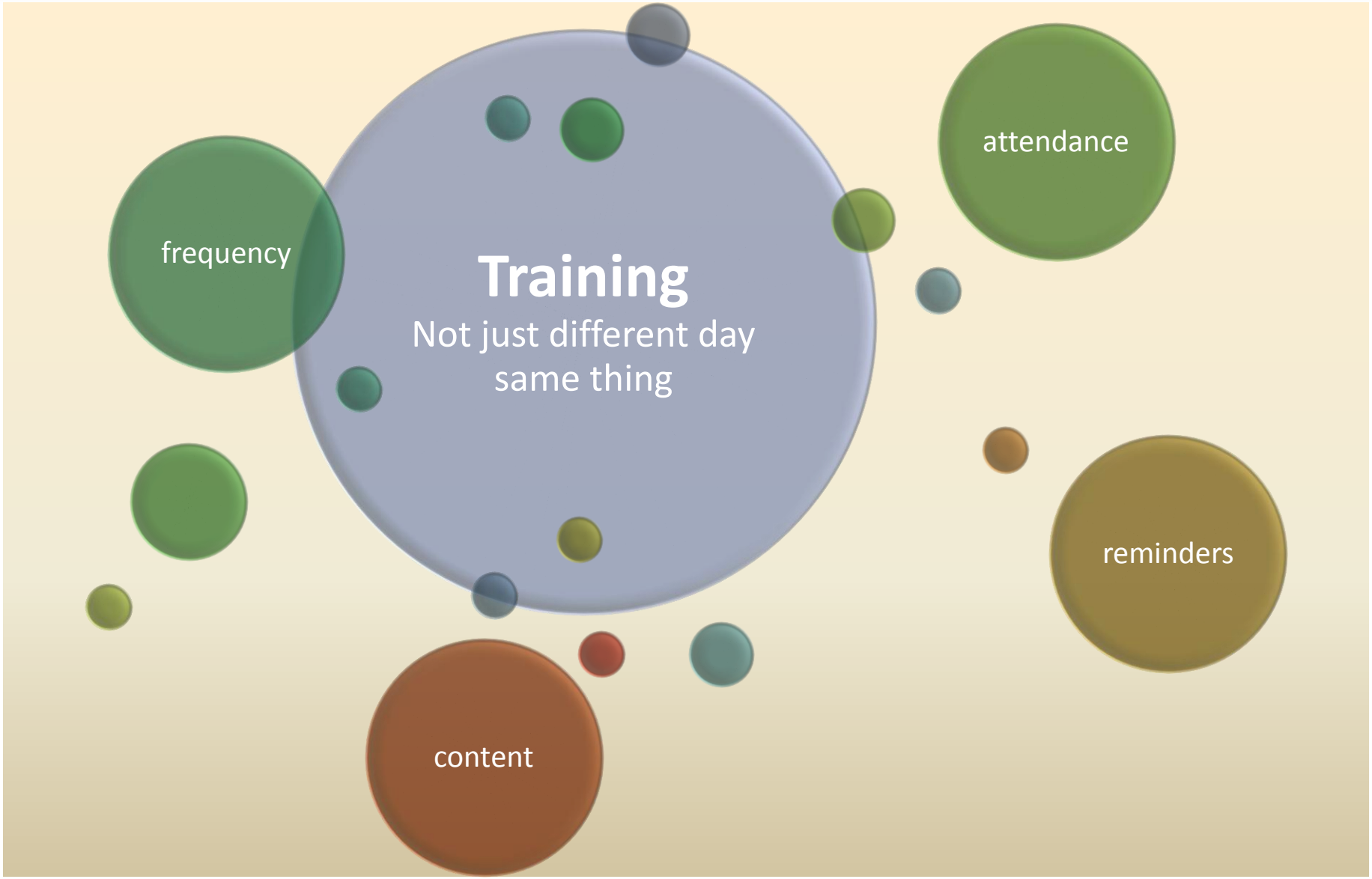
- KHIE must assess risk and mitigate

HIPAA Complaints

Who can file a HIPAA complaint?

Anyone who believes there has been a HIPAA violation can file a complaint with HHS up to 180 days after they first become aware of the perceived lack of compliance and they can go back six years. 45 CFR 160.306

Training


Training
Not just different day
same thing
attendance
frequency
reminders
content

GOEHI AND KHIE EMPLOYEE POLICIES

Manage the Privacy Rule by use of Policies and Procedures

http:KHIE.ky.gov

KHIE

http://www.chfs.ky.gov/os/oats/policies.htm

OATS

http://technology.ky.gov/governance/Pages/policies.aspx

COT

First fine for less than 500 records

Hospice of North Idaho

- 440 records
- Lost laptop

No risk assessment therefore no appropriate measures to address the risk or to maintain the appropriate security measures.

$50,000 fine, Corrective Action Plan

CAP required employer to enforce policies and sanction policy violations

KHIE
KENTUCKY HEALTH INFORMATION EXCHANGE

Los Angeles Times

UCLA pays $865,500 to settle celebrity medical record snooping case

July 7, 2011

"Settlement with U.S. regulators also call for UCLA to retrain staff and take steps to prevent future breaches. Some staff have already been fired for viewing the records of Farrah Fawcett, Michael Jackson and others."

UCLA Health System has agreed to pay $865,500 as part of a settlement with federal regulators announced Thursday after two celebrity patients alleged that hospital employees broke the law and reviewed their medical records without authorization.

Federal and hospital officials declined to identify the celebrities involved. The complaints cover 2005 to 2009, a time during which hospital employees were repeatedly caught and fired for peeping at the medical records of dozens of celebrities, including Britney Spears, Farrah Fawcett and then-California First Lady Maria Shriver.

The employee was not named in the agreement, and the hospital spokeswoman declined to identify who it was. But the timing and description of the alleged violations cited in the agreement suggest that it may have been Lawanda Jackson, an administrative specialist at Ronald Reagan UCLA Medical Center who was fired in 2007 after she was caught accessing Farrah Fawcett's medical records and allegedly selling information to the National Enquirer.

Jackson later pleaded guilty to a felony charge of violating federal medical privacy laws for commercial purposes but died of cancer before she could be sentenced. Fawcett died of cancer in 2009.

Office of Civil Rights

Part of the U.S. Department of Health and Human Services

Enforces civil rights from health care providers receiving federal financial assistance from HHS, one of the most active federal regulators

- Where does your data reside?
- Who has access to PHI?
- How do you restrict access to PHI?
- How does your agency train your employees?

Office for Civil Rights

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2010	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2009	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints to Covered Entity
2008	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints to Covered Entity
2007	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2006	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Notice
2005	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Mitigation
2004	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Authorizations
partial year 2003	Safeguards	Impermissible Uses & Disclosures	Access	Notice	Minimum Necessary